ELEVATE LABS CYBER SECURITY INTERNSHIP

Task-6:

1.Create multiple passwords with varying complexity.

Password	Strength	Why
qwerty	Very Weak	All lowercase, simple keyboard pattern, very easy to guess.
qwerty123	Weak	Adds numbers, but still very common and easily guessed.
Qw3rty!	Moderate	Mix of uppercase, lowercase, number, and symbol but too short.
Qw3rty!92@	Strong	Longer and includes a mix of characters, harder to crack.
Qw3_rT9!$eY@72	Very Strong	Long (14+ characters), uses all character types, less predictable.
7&Qw3$Ty!_r91*Kz	Ultra Secure	16+ characters, high randomness, excellent security.

2.Use uppercase, lowercase, numbers, symbols, and length variations.

Password	Score	Time to Crack	Feedback
qwerty	**Very Weak**	**Instant**	**Common password, easy to guess, only lowercase.**
qwerty123	**Weak**	**<1 second**	**Frequently used, predictable sequence.**
Qw3rty!	**Moderate**	**Few hours**	**Good mix, but too short for strong security.**
Qw3rty!92@	**Strong**	**Centuries**	**Strong due to length and character mix.**
Qw3_rT9!$eY@72	**Very Strong**	**Trillions of years**	**Excellent randomness, hard to guess.**
7&Qw3$Ty!_r91*Kz	**Extremely Strong**	**Longer than the universe**	**Ideal password: long, random, all character types.**

3.Test each password on password strength checker.

- Use at least 12 to 16 characters.
- Include uppercase, lowercase, numbers, and special characters.
- Avoid common words or sequences like 12345, password, or your name.
- Don’t reuse passwords across different accounts.
- Try using passphrases — a mix of random words (e.g., Tree$Moon!Car#92).
- Use a password manager to store and generate strong passwords.
- Always enable two-factor authentication (2FA) where possible.

4.Note scores and feedback from the tool.

- Length is more important than complexity alone.
- Randomness and unpredictability greatly improve password strength.
- Simply replacing letters with symbols (like @ for a) is not enough.
- Reusing the same password across platforms is risky.
- Passwords should be unique, strong, and preferably managed using a tool.
- Passphrases are easy to remember and strong if random enough.

5.Identify best practices for creating strong passwords:

Attack Type	**Description**
Brute Force	Tries every possible combination until the password is cracked.
Dictionary Attack	Uses lists of common passwords or phrases to guess quickly.
Credential Stuffing	Uses previously leaked passwords to log in to different accounts.
Phishing	Tricks users into revealing passwords via fake emails or websites.
Keylogging	Malware records everything typed on the keyboard, including passwords.

6.Write down tips learned from the evaluation.

Password complexity makes it **much harder** for attackers to crack your password. A weak password like qwerty123 can be guessed in seconds, but a complex one like 7&Qw3$Ty!_r91*Kz could take **trillions of years** to break with current technology.

- Longer + Random + Mixed characters = More secure.
- Password strength is your **first line of defense** in cybersecurity.

7.Research common password attacks (brute force, dictionary).

1. **Brute Force Attack**: The attacker tries all possible combinations until they guess your password. Longer and more complex passwords take a very long time to crack this way.
2. **Dictionary Attack**: The attacker uses a list of common passwords and word combinations (like password, p@ssw0rd, 123456) to try and guess your password quickly.
3. **Credential Stuffing**: Hackers use leaked usernames and passwords from other websites to try and log into your other accounts — especially if you use the same password everywhere.
4. **Phishing**: Hackers trick you into giving your password by sending fake emails or creating fake websites that look real.
5. **Keylogging**: A virus or malware records everything you type on your keyboard — including your passwords — and sends it to the hacker.

8.Summarize how password complexity affects security.

- Change your passwords regularly, especially for critical accounts.
- Avoid using the same password for work and personal accounts.
- Watch out for fake login pages (phishing).
- Log out from public/shared devices.
- Enable alerts for suspicious login attempts when possible.